REMARKS

This application has been reviewed in light of the Office Action dated September 24, 2007. Claims 1-17, 19, and 20 are presented for examination, of which Claims 1, 15, and 17 are in independent form. Claims 1, 15, and 17 have been amended to define Applicants' invention more clearly. Claim 18 has been canceled without prejudice or disclaimer of the subject matter presented therein. Favorable reconsideration is requested.

The Office Action rejected Claims 1-7, 9-12, and 14-18 under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 6,671,358 (*Seidman et al.*, hereinafter "*Seidman*"), as supported by U.S. Provisional Application 60/286,309 (*Seidman et al.*, hereinafter "*Seidman_P*"), in view of U.S. Patent No. 6,445,794 (*Shefi*); rejected Claims 8 and 13 under § 103(a) as being unpatentable over *Seidman*, as supported by *Seidman_P*, in view of *Shefi*, and in further view of Official Notice; and rejected Claims 19 and 20 under § 103(a) as being unpatentable over *Seidman*, as supported by *Seidman_P*, in view of *Shefi*, in further view of U.S. Patent No. 6,438,235 (*Simms III*, hereinafter "*Simms*"). Applicants respectfully traverse the rejections and submit that amended independent Claims 1, 15, and 17, together with the claims dependent therefrom, are patentably distinct from the cited art for at least the following reasons.

Amended Claim 1 recites, in part, "the transaction device is validated based at least in part on both the transaction device identifier and the transaction device authentication tag, both having been received from the RFID transaction device; and wherein the transaction device random number is used to lookup a previously stored decryption key for decrypting at least one of the transaction device identifier and the

transaction device authentication tag, the transaction device random number having been received from the RFID transaction device" (emphasis added).

The Office Action admits that *Seidman* does "not explicitly disclose a system comprising a transaction device random number generator for generating a transaction device random number; wherein the transaction device is validated based at least in part on the transaction device identifier and the transaction device random number . . . ." *See* the Office Action, the paragraph bridging pages 2 and 3. Indeed, Applicants have found nothing in *Seidman* to teach or reasonably suggest such features. As previously discussed in the Amendment of January 24, 2008, *Seidman* does not appear to be concerned with any form of transaction device validation through the use of a random number. The Office Action then looks to *Shefi* as disclosing such features. *See* the Office Action, page 3.

Shefi appears to provide a system for "secure communication over an insecure channel, or for secure identification" using "one-time pads." *See Shefi* Col. 10, lines 60-62. As best understood by Applicants, to provide a "forgery-resistant identification of a subject [device]," *Shefi* encrypts an identifier for the subject device 24 by merging the identifier for the subject device 24 with at least one number from the generated one-time pad. *See Shefi* Col. 17, lines 42-47 and Col. 18, lines 17-30. The encrypted identifier is then sent from subject device 24 to access device 26 and the access device 26 then decrypts the encrypted identifier using an identical copy of the one-time pad used at the subject device 24. *See Shefi* Col. 16, lines 20-27 and Col. 18, lines 31-34. "Access device 26 could then check the identifier against a list of identifiers for subject devices 24" to determine whether the identify of subject device 24 is legitimate. *See Shefi* Col. 18, lines 34-41.

Nothing has been found in *Shefi* to teach or reasonably suggest "the transaction device is validated based at least in part on both the transaction device identifier and the transaction device authentication tag, both having been received from the RFID transaction device" much less teach or reasonably suggest, "wherein the transaction device random number is used to lookup a previously stored decryption key for decrypting at least one of the transaction device identifier and the transaction device authentication tag, the transaction device random number having been received from the RFID transaction device," as recited by amended Claim 1 (emphasis added).

Furthermore, *Simms* fails to cure the aforementioned deficiencies of *Seidman* and *Shefi*. *Simms* appears to determine the validity of a private key utilized within a chip "by generating a random number, encrypting it with the public key, sending the encrypted information to the chip, allowing the chip to decrypt the random number using the private key, and again encrypt the random number using the private key. If the random number is presented by decrypting the returned encrypted string with the public key, there must be a valid private key utilized within the chip." *See Simms* Col. 8, lines 60-67. Nothing has been found in *Simms* to teach or reasonably suggest the aforementioned features of amended Claim 1.

For at least these reasons, Applicants submit that the Office cannot sufficiently establish a *prima facie* case of obviousness against amended Claim 1, and that the various proposed combinations of *Seidman*, *Shefi*, *Simms*, and other concepts alleged by the Office to be well known at the time of Applicants' invention, even if deemed legally permissible or technically feasible, would fail to arrive at the system for securing a Radio Frequency (RF) transaction of Claim 1. Accordingly, the rejection under 35 U.S.C § 103(a) is deemed obviated, and its withdrawal is respectfully requested.

Independent Claims 15 and 17 include some features similar to those discussed above with respect to Claim 1. Therefore, those claims are also believed to be patentable under a similar rationale as discussed above.

Furthermore, amended independent Claim 17 includes a transaction device reader that passes data between a transaction device and an account issuer associated with the transaction device. One of feature of Claim 17 includes validating both the transaction device and the transaction device reader at the account issuer using the same random number generated at the transaction device. Nothing has been found in the various proposed combinations of *Seidman*, *Shefi*, *Simms*, and other concepts alleged by the Office to be well known at the time of Applicants' invention to teach or reasonably suggest such a feature. For at least this additional reason, Applicants submit that the Office cannot sufficiently establish a *prima facie* case of obviousness against amended Claim 17.

The other rejected claims in this application depend from one or another of the independent claims discussed above and, therefore, are submitted to be patentable for at least the same reasons. Since each dependent claim also is deemed to define an additional aspect of the invention, individual reconsideration of the patentability of each claim on its own merits is respectfully requested.

Applicants' undersigned attorney may be reached in our New York office by telephone at (212) 218-2100. All correspondence should continue to be directed to our below listed address.

Respectfully submitted,

/Jonathan Berschadsky/
Jonathan Berschadsky
Attorney for Applicants
Registration No. 46,551

FITZPATRICK, CELLA, HARPER & SCINTO
30 Rockefeller Plaza
New York, New York 10112-3801
Facsimile: (212) 218-2200

FCHS_WS 2000246_1